REMARKS/ARGUMENTS

The Examiner rejected priorly presented claims 1-15 as unpatentable, 35 USC 103(a), over Poier et al. patent application US 2002/0124090 A1, August 20, 2001 (hereinafter Poier) in view of Murakawa US 2001/0020273 A1, December 1, 2000 (hereinafter Murakawa). In response thereto, applicants have amended independent claims 1, 8, and 12 to more clearly recite applicants' invention.

Applicants' invention is directed at situations where a first device on a local network is separated from an external/public network by an access blocking apparatus (e.g., firewalls and network address translators (NATs)) that prevents second devices external to the local network from communicating with the first device without first reconfiguring the blocking apparatus (Specification, page 1, line 12 to page 2, line 3). In accordance with applicants' invention, methods and systems allow such communications to occur without having to perform these reconfigurations. Specifically, applicants' invention as recited by amended independent claim 1 is a method performed by a hub that enables a second device to bypass an access blocking apparatus and communicate with a first device when the first device is on a local network that comprises the access blocking apparatus, which apparatus connects the local network to external networks and separates the first and second devices. The hub terminates a virtual pipe from the first device, assigns an IP address to the first device, and then associates the IP address with the virtual pipe. Communications originated by the second device are addressed to the first device using this IP address. Accordingly, the hub receives the communications, routes them to the virtual pipe and then tunnels the communications over the virtual pipe to the first device, thereby bypassing the access blocking apparatus. As a result, because of the virtual pipe established between the hub and the first device, the second device is able to originate communications to the first device without having to reconfigure the access blocking apparatus.

The Examiner indicates that Poier in combination with Murakawa teach claim 1. Applicants respectfully disagree because Poier fails to teach or suggest a hub that terminates a virtual pipe from a first device and tunnels communications over this virtual pipe from a second device in order to bypass access blocking apparatus and thereby enable communications from the second to the first device, as the Examiner indicates. In addition, there is no motivation, including the Examiner's proposed motivation for improved security, to combine Poier and Murakawa since none of the teachings are directed to the problem of enabling communication in the presence of blocking apparatus without first reconfiguring the blocking apparatus. Furthermore, applicants' are unclear why combining Murakawa with

communications. In this case, the VPN is between the gateway and the node 12b. Again, the centralized server here only plays the role of configuring the nodes and gateway to correctly establish the VPN but does not play a role in bypassing the gateway in order for the nodes to communicate. (Poier, paragraphs 49). Note also that the gateway 24 is not the same as the node of claim 1. Most significantly, there is no virtual pipe between the gateway 24 and the node 25 on the local network through which communications from the node 12b are being routed. In other words, the gateway is not terminating a virtual pipe from a first device on a local network and routing communications from a second device through this virtual pipe, thereby bypassing an access blocking apparatus and enabling communications.

Lastly, applicants note that the Examiner makes specific reference to Poier, paragraph 10, with respect to the step of terminating virtual pipes. In paragraph 10, Poier is making brief reference to prior art nodes that terminate VPNs. However, applicants are unclear as to the relevance of paragraph 10 because Poier fails to subsequently teach how the methods performed by these prior art nodes and the methods performed by the nodes of Poier teachings are combined to realize applicants' invention. Accordingly, Poier fails to teach or suggest claim 1 as the Examiner specifies.

Turning to Murakawa, Murakawa is concerned with an environment where a device on a wide area network (WAN) (hereinafter "WAN device") needs to securely convey information over the WAN to a device on a local area network (LAN) (hereinafter "LAN device"). Murakawa teaches that a security gateway typically connects the LAN to the WAN. In order for the WAN device to securely communicate over the WAN to the LAN device, the WAN device establishes a VPN with the gateway. However, Murakawa indicates that even though the communications over the WAN are now secure, because the WAN device has a WAN-based IP address that is external to the LAN, configurations must still be performed on the LAN devices to give the WAN device access. If these configurations are not properly performed, security issues can arise. (Murakawa, paragraphs 2-5 and 36-41). Accordingly, Murakawa teaches a method by which the WAN device virtually appears as a device on the LAN thereby avoiding the configuration of the LAN devices. Specifically, in accordance with Murakawa, when the VPN is established between the WAN device and the gateway, the gateway also assigns the WAN device a secondary IP address that is local to the LAN. A LAN device and the WAN device use this secondary IP address to process all communications, while the WAN device's actual WAN-based IP address is used to tunnel the communications over the VPN. (Murakawa, paragraphs 58-84).

Murakawa further teaches in paragraphs 93-98 that the above-described gateways often use NAT technology to configure the LAN with private IP addresses. Murakawa notes

that the NAT technology usually prevents a WAN device from accessing LAN devices. With respect to assigning a secondary IP address to a WAN device, Murakawa teaches that the NAT related issues are overcome by using the NAT technology to assign the WAN device one of the private IP addresses of the LAN, again, making the WAN device virtually appear as though it is on the LAN.

The Examiner indicates that Murakawa teaches the IP assigning and associating steps of claim 1 and that improved security would motive one to combine the teachings of Poier and Murakawa to obtain applicants' invention as recited by claim 1. First, applicants' are not clear why improved security would motivate this combination because none of the issues addressed by applicants' invention as recited by claim 1, Poier's teachings, or Murakawa's teachings deal with improved security. Applicants' invention is directed at bypassing an access blocking apparatus. Poier is directed at configuring VPNs through a central server. As for Murakawa, the teachings recognize the existence of VPNs to provide security and show how the use of secondary IP addresses can prevent the need to perform certain VPN configurations that can compromise security; however, Murakawa does not directly teach the use of IP addresses to actually provide additional security. Second, applicants are unclear as to why assigning secondary IP addresses to the connections between nodes and the central server of Poier would directly or indirectly improve security. Third, disregarding the security issue, it is not clear what benefit at all secondary IP addresses add to Poier since Poier is not directed at communicating through the central server. The secondary IP addresses would only unnecessarily complicate Poier's teachings.

Note also that Murakawa alone fails to anticipate or obviate amended claim 1. Specifically, Murakawa teaches that the device on the WAN\external network establishes the virtual pipe to the gateway and that the WAN device\VPN are assigned the new IP address while claim 1 recites that the device on the local network establishes the virtual path and is assigned the secondary IP address. This difference is significant and non-obvious for several reasons. First, Murakawa teachings and claim 1 are directed at overcoming different problems. In particular, Murakawa is directed at overcoming the configuration issues created when using VPNs across WANs to give WAN devices secure access to LANs. On the contrary, applicants' invention is directed at allowing an external device to access a local device while bypassing the issues access blocking apparatus create. Accordingly, Murakawa fails to suggest configuring the VPN from the local device and assigning this device a new address because this would be divergent from Murakawa's original intent of securing access over the WAN. Second, Murakawa's teachings fail to overcome the problem claim 1 resolves

because Murakawa does not bypass the gateway/NAT (i.e., accessing blocking device) but actually employs this technology to realize the method, as described above.

Turing to dependent claims 2 –7, these claims depend on amended claim 1 and are novel and nonobvious for the same reasons as set forth above.

Amended claim 8 recites a system for bypassing an access blocking apparatus and thereby enabling communications between a first device and a second device wherein the first device is on a local network and the second device is external to the local network, the local network including the access blocking apparatus that connects the local network to external networks and that separates the first and second devices. The system comprises a secure hub and a virtual pipe between the first device and the secure hub. The secure hub includes an IP address pool from which an IP address can be assigned to the first device, means for associating the assigned IP address with the virtual pipe, means for routing communications from the second device and addressed to the first device to the virtual pipe, and means for tunneling the communications over the virtual pipe to the first device thereby bypassing the access blocking apparatus

The Examiner indicates that Poier's centralized server and secure connections between nodes and this centralized server are the same as the secure hub and the virtual pipe between this secure hub and the first device of claim 8, and that Poier's centralized server includes means for tunneling communications over the secure connections to the nodes, similar to claim 8. Applicants respectfully disagree because Poier fails to teach or suggest that the described combination of a centralized server and nodes are a system for bypassing access blocking apparatus and thereby enabling communications between a first device and a second device as claim 8 recites. Again, although there are secure connections between nodes and the centralized server, there is also a VPN between the nodes. This VPN is used by the nodes to communicate and never traverses the centralized server. In addition, when an access blocking apparatus, such as a NAT, separates the nodes, the centralized server does not play a role in the actual transfer of data to bypass the NAT. (Poier, paragraphs 50-51). The NAT actually manipulates packets as they traverse the NAT (Poier, paragraph 53), contrary to applicants' invention.

As for Murakawa, again, there is no motivation for combining Poier and Murakawa. Similarly, Murakawa alone fails to teach or suggest amended claim 8 because Murakawa teaches that the device on the WAN\external network establishes the virtual pipe to the gateway and that the WAN device\VPN are assigned the new IP address while claim 8 recites that the device on the local network establishes the virtual path and is assigned the secondary

IP address. Again, these differences are significant and non-obvious for the reasons set forth above.

Dependent claims 9-11 depend on amended claim 8 and are novel and nonobvious for the same reasons as set forth above.

Amended claim 12 recites a system for enabling communication from a second communication device, which is external to a local network, through the public network and bypassing a security access blocking apparatus to a first communication device on the local network, wherein the security access blocking apparatus provides the first communication device access to the public network and separates the first and second communication devices. The system comprises a secure hub and means for creating a virtual pipe between the secure hub and the first communication device for tunneling communication and bypassing the security access blocking apparatus, wherein the secure hub further includes means for assigning an IP address to the first communication device and associating the IP address with the virtual pipe.

Again, the combination of Poier and Murakawa fail to teach or suggest amended claim 12. Poier's combination of a secure connection between nodes and a centralized server are divergent from a system comprising a secure hub and means for creating a virtual pipe between the secure hub and the first communication device for tunneling communication and bypassing a security access blocking apparatus, as claim 12 recites Poier teaches that there is an additional VPN between the nodes for communicating, which VPN does not traverse the centralized server. When this VPN traverses access blocking apparatus, such as a NAT, packets are actually manipulated by the NAT rather than bypassing the NAT as claim 12 recites.

As for Murakawa, again, there is no motivation for combining Poier and Murakawa. Similarly, Murakawa alone fails to teach or suggest amended claim 12 because claim 12 recites that the virtual connection is between the secure hub and the device behind the access blocking apparatus rather than between a gateway and the device on the public network as Murakawa teaches. Again, this difference is significant and non-obvious for the reasons set forth above. Similarly, claims 13-15, which depend from claim 12, are also novel and nonobvious in view of Poier and Murakawa.

Since Poier and Murakawa singly or in combination do not teach or suggest applicants' novel methods and apparatus as set forth in applicants' amended claims, applicants submit that claims 1-15 are clearly allowable. Favorable consideration and allowance of claims 1-15 are therefore requested.

Applicants earnestly believe that this application is now in condition to be passed to issue, and such action is also respectfully requested. However, if the Examiner deems it would in any way facilitate the prosecution of this application, he is invited to telephone applicants' agent at the number given below.

Respectfully submitted,
Telcordia Technologies, Inc.

By: 
Glen Farbanish
Reg. No. 50561
Tel.: (732) 699-3668